Electronic Version
Stylesheet Version v1.1.1

Secure Credit Card Employing Pseudo-Random Bit Sequences for Authentication

Abstract

A secure credit card has a pair of linear feedback shift registers (LFSRs) for generating a pair of random numbers. The LFSRs each have a unique initial state and feedback tap configuration. Hence, they each produce a unique sequence of numbers. When a financial transaction occurs, the LFSRs are operated for a random number of clock cycles, to create a pair of matched random numbers. Each card issued has unique LFSR settings, and so will produce characteristic random numbers. At a financial institution, the LFSR settings are known, so the financial institution can determine by calculation if the pair of random numbers is authentic. There are many variations, including a credit card with a secret security code for activation, and 2-way "handshake" communication with the financial institution. Also, one of the LFSRs may be replaced with a binary, or similar counter.